What is claimed is:

1   1.   A method comprising:

2   receiving a request from a device across a public network

3   at a first network component to establish a connection between

4   the device and a private network;

5   determining if the device is authorized to connect with

6   the private network;

7   if authorized, forwarding the request from the first

8   network component to a second network component; and

9   the second network component creating a connection

10   between the private network and the device via the first

11   network component.

1   2.   The method of claim 1 further comprising the second

2   network component establishing a temporary connection between

3   the device and a device included in the private network.

1   3.   The method of claim 1 further comprising, if not

2   authorized, denying the device access to the private network.

1   4.   The method of claim 1 in which the private network

2   is separated from the public network by a security mechanism.

1   5.   The method of claim 1 in which the first network

2   component and the second network component have a connection

3   lasting as long as a mechanism at each of the components

4   supporting the connection remains active.

1   6.   The method of claim 1 in which the first network

2   component and the device have a connection lasting as long as

3   a mechanism at the first network component and a mechanism at

4   the device supporting the connection remain active.

1   7.   The method of claim 1 in which the determining

2   includes authenticating a password.

1   8.   The method of claim 1 in which the public network

2   includes the Internet.

1   9.   The method of claim 1 in which the first network

2   component and the second network component include proxy

3   servers.

1   10.   An article comprising a machine-readable medium

2   which stores machine-executable instructions, the instructions

3   causing a machine to:

4   receive a request from a device across a public network

5   at a first network component to establish a connection between

6   the device and a private network;

7   determine if the device is authorized to connect with the

8   private network;

9   if authorized, forward the request from the first network

10   component to a second network component; and

11   create, with the second network component, a connection

12   between the private network and the device via the first

13   network component.

1   11.   The article of claim 10 further comprising the

2   second network component establishing a temporary connection

3   between the device and a device included in the private

4   network.

1   12.   The article of claim 10 further comprising, if not

2   authorized, denying the device access to the private network.

1   13.   The article of claim 10 in which the private network

2   is separated from the public network by a security mechanism.

1   14.   The article of claim 10 in which the first network

2   component and the second network component have a connection

3   lasting as long as a mechanism at each of the components

4   supporting the connection remains active.

1   15.   The article of claim 10 in which the first network

2   component and the device have a connection lasting as long as

3   a mechanism at the first network component and a mechanism at

4   the device supporting the connection remain active.

1   16.   The article of claim 10 in which the determining

2   includes authenticating a password.

1   17.   The article of claim 10 in which the public network

2   includes the Internet.

1   18.   The article of claim 10 in which the first network

2   component and the second network component include proxy

3   servers.

1   19.   A system comprising:

2   a device configured to connect to a public network;

3   a server component configured to connect to the public

4   network; and

5   an agent component configured to connect to the server

6   component and to a private network separated from the public

7   network by a security mechanism and configured to provide the

8   device with access to the private network via the server

9   component and the public network.

1   20.   The system of claim 19 in which the agent component

2   is also configured to provide any number of devices configured

3   to connect to the public network with access to the private

4   network via the server component and the public network.

1   21.   The system of claim 19 in which the agent component

2   is also configured to provide the device with access to a

3   device included in the private network.

1   22.   The system of claim 19 in which the server component

2   and the agent component are both extensible to support any

3   protocols used by the public network and by the private

4   network.

1   23.   The system of claim 19 in which the public network

2   includes the Internet.

1   24.   The system of claim 19 in which the server component

2   is also configured to authenticate the device.

1   25.   The system of claim 19 in which the agent component

2   is also configured to maintain a connection with the server

3   component as long as a mechanism at each of the components

4   supporting the connection remains active.

1   26.   The system of claim 19 in which the server component

2   is also configured to maintain a connection with the device as

3   long as a mechanism at the server component and a mechanism at

4   the device supporting the connection remain active.

1   27.   The system of claim 19 in which the agent component

2   is implemented on at least one of the security mechanisms.

1   28.   The system of claim 19 in which the agent component

2   is implemented inside the private network.

1   29.   The system of claim 19 in which the server component

2   and the agent component are both implemented on at least one

3   of the security mechanisms.